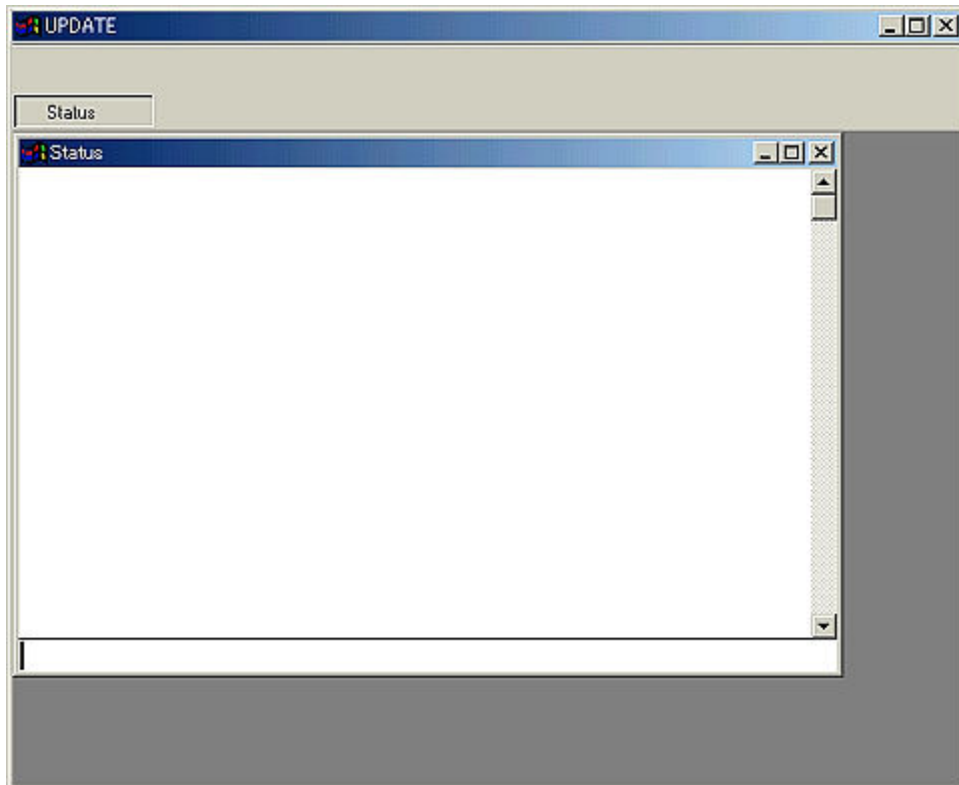


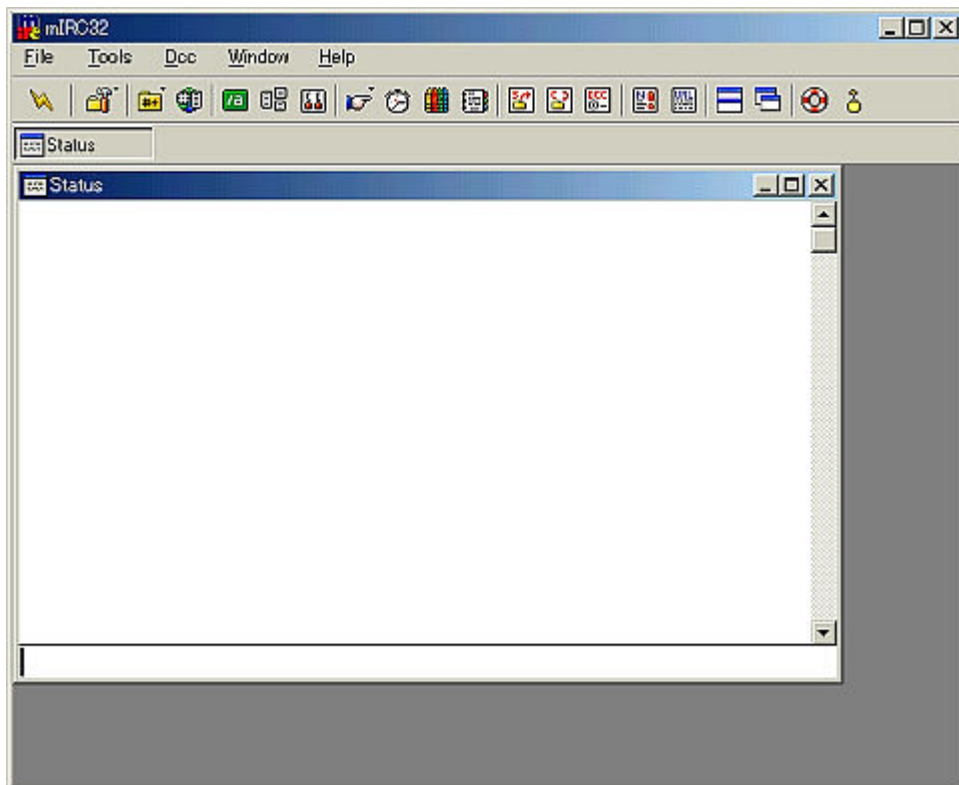
## ウィルス解析報告書

ウイルス名	Win-Troj/MircPack.597504
プログラム名 及び容量 (添付ファイル名)	explorer.exeほか 597504バイト
種別	トロイの木馬補助プログラム(トロイの木馬に利用するため、mIRCバージョン5.91を改造したもの)
プログラム言語	ポーランドC++
発症環境	Windows95/98/ME/NT/2000/XP
発見日時	2002年11月18日
発見場所 (発信地)	不詳
危険性	やや危険(5段階で2以下)
発症条件	32ビットWindows環境において、トロイの木馬が実行され、インストールされたとき。
	<p>このプログラムは、トロイの木馬を構成する一つのパーツとして作成されている。</p> <p>この正体はmIRCと呼ばれるIRCクライアントプログラムのバージョン5.91を改造したものである。mIRCのバージョン5シリーズはセキュリティの点でいくつかの弱点を持っていたが、それは現在リリースされているバージョン6において改善されている。</p> <p>過去において、ワームやトロイの木馬から利用されていたmIRCバージョン5であったが、最新バージョンではそういった利用が困難になったため、「それならばセキュリティホールのあるmIRCバージョン5をも含んだ形でトロイの木馬を構成しよう」という、ウイルス作者の発想から作成されたものと思われる。</p> <p>改造点は、プログラムの画像やメニューを削除し、実行型圧縮プログラムによって圧縮してある点である。トロイの木馬は、この改造mIRCをトロージャン動作の下請け(主にIRC通信部分とスクリプトエンジン)として利用するわけである。</p> <p>このプログラムを単独で動作させたとき、mIRCバージョン5.91を動作させたときの画面を下記に示す。このプログラムがmIRCを改造したものであることが、下図を見ても歴然である。</p>
	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">About mIRC</p> <p>mIRC_ v5.91 32bit An Internet Relay Chat Client</p> <p>Copyright _ 1995-2001 mIRC Co. Ltd. All Rights Reserved.</p> <p>Written by Khaled Mardam-Bey <span style="float: right;">Author!</span></p> <p>Licensed to: Unlicensed Copy</p> <p style="text-align: center;"> <input type="button" value="Introduction"/> <input type="button" value="How to register"/> </p> <p>Please visit the mIRC website for the latest version, hints and tips, and general IRC information.</p> <p><input checked="" type="checkbox"/> <input type="button" value="http://www.mirc.com"/> <input type="button" value="Visit"/></p> </div> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">About mIRC</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>mIRC_ v5.91 32bit An Internet Relay Chat Client</p> <p>Copyright _ 1995-2001 mIRC Co. Ltd. All Rights Reserved.</p> <p>Written by Khaled Mardam-Bey <span style="float: right;">Author!</span></p> </div> </div> <p>Licensed to: Unlicensed Copy</p> <p style="text-align: center;"> <input type="button" value="Introduction"/> <input type="button" value="How to register"/> </p> <p>Please visit the mIRC website for the latest version, hints and tips, and general IRC information.</p> <p><input checked="" type="checkbox"/> <input type="button" value="http://www.mirc.com"/> <input type="button" value="Visit"/></p> </div> </div>
	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;">Win-Troj/MircPack.597504を単独動作させた場合</div> <div style="width: 45%;">mIRCバージョン5.91を単独動作させた場合の起動ダイアログ</div> </div>



Win-Troj/MircPack.597504を単独動作させた場合

ウイルスの活動、影響



mIRCバージョン5.91を単独動作させた場合

被害の規模

不明

亜種、変種の有無

いくつかの亜種が存在するとされているが詳細は不明

このプログラムは、mIRCバージョン5.91からメニューリソースと画像リソースを取り除き、実行型圧縮プログラムによって圧縮を施したものである。

ウイルス動作概要	メニューリソース等が無いため、通常のIRCクライアントとして利用することは不可能であり、そういう意味からもトロイの木馬と判断されているが、あくまで内容はmIRCである。したがって、動作はmIRCに準ずる。なお、フローチャートは提供不可能である。
感染・発症防止方法	アプリケーションはオリジナルCDまたはネット上の一次配布場所から入手し、トロイの木馬のおそれのある入手経路不明なプログラムは利用しない。
ウイルスの駆除方法	< 確認 > 597,504バイトのファイルを検索し、それを実行した場合に、画像リソースを失ったmIRCが起動した場合は、このトロイの木馬補助プログラムである。 < 駆除 > 上記で確認されたファイルを削除する。
その他	報告書作成 : 2003年2月1日現在